IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Applicants: **Jonathan TAMS, Mark A. PEARCE, Robin IDDON, Ronnie BROWN**

Case: **3Com-7/Con(1611.NMD.US.C)**

Serial No.: Filed:

Group Art Unit: **2153**

Examiner: **Kenneth Fields**

Title: **METHODS AND APPARATUS FOR MONITORING, COLLECTING, STORING, PROCESSING AND USING NETWORK TRAFFIC DATA OF OVERLAPPING TIME PERIODS (as amended)**

Commissioner for Patents
BOX PATENT APPLICATION
Washington, D. C. 20231

S I R:

PRELIMINARY AMENDMENT

Please amend the above-identified patent application, filed simultaneously herewith, as follows:

IN THE TITLE-

Delete the title and replace with:

--METHODS AND APPARATUS FOR MONITORING, COLLECTING, STORING, PROCESSING AND USING NETWORK TRAFFIC DATA OF OVERLAPPING TIME PERIODS--.

IN THE CLAIMS-

To facilitate entry of the following changes, the Applicants have submitted herewith substitute pages providing all the pending claims, as they now stand, incorporating the changes indicated below.

Please cancel claim 7.

Rewrite the following claims:

--1. (Amended) A method of processing and storing data in a computer system including processor circuitry, and a data storage device, the method comprising the steps of:

storing first and second sets of records in separate first-in, first-out data structures, respectively, on the data storage device, the first and second sets of records being of different data resolutions and corresponding to overlapping periods of time;

operating the processor circuitry to receive data collected over a period of time; and

operating the processor circuitry to update, in parallel, at least one record in each of the stored first and second sets of records with the received data such that a previous record included in each of the first and second data structures is replaced.

12. (Amended) A method of collecting and processing network traffic data, comprising the steps of:

periodically collecting network traffic data from a data probe,

generating a database of network traffic information from the collected network traffic data, the database comprising a plurality of network traffic data sets of differing degrees of data resolution corresponding to overlapping network traffic time periods,

storing each of the plurality of network traffic data sets in a different first-in, first-out data structure wherein a limited amount of data storage space is used for each of the different first-in, first out data structures,

updating, in parallel, at least one record in the different first-in, first-out data structures with the collected network traffic data, and

overwriting the oldest data records in the first-in, first-out data structure used to store one of the network traffic data sets, when the limited amount of data storage space used for said first-in, first-out data structure is filled with records.

17. (Amended) A system for monitoring network traffic data, comprising:

a plurality of network traffic data probes for collecting network traffic information;

processor circuitry coupled to the network traffic probes for receiving data therefrom; and

a data storage device for storing a network traffic database generated by the processor circuitry using data collected by the network traffic data probes, the data storage device including:

a plurality of data structures, each data structure being a first-in, first-out data structure, each one of the plurality of data structures including network traffic data:

a) stored at a different resolution than the resolution at which network traffic data is stored in the other ones of the plurality of data structures; and

b) corresponding to a period of time which overlaps the period of time for which network traffic data is stored in the other ones of the plurality of data structures;

means for updating, in parallel, at least one record in the different first-in, first-out data structures with the collected network traffic data, and

means for overwriting the oldest data records in the first-in, first-out data structure used to store one of the network traffic data sets, when the limited amount of data storage space used for said first-in, first-out data structure is filled with records. --.

REMARKS

If the Examiner believes that there are any unresolved issues preventing allowance in any of the claims now pending in the application, the Examiner should telephone Ms. Janet M. Skafar, Esq. at (650) 988-0655 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

March 30, 2001

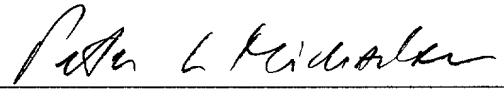
Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671

MICHAELSON & WALLACE
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

*****EXPRESS MAIL CERTIFICATION*****

"Express Mail" mailing label number: **EL632365012US**
Date of deposit: **April 2, 2001**

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, **Box Patent Application,** Washington, D.C. 20231.



Signature of person making certification

Peter L. MICHAELSON
Name of person making certification

What is claimed is:

1. A method of processing and storing data in a computer system including processor circuitry, and a data storage device, the method comprising the steps of:

storing first and second sets of records in separate first-in, first-out data structures, respectively, on the data storage device, the first and second sets of records being of different data resolutions and corresponding to overlapping periods of time;

operating the processor circuitry to receive data collected over a period of time; and

operating the processor circuitry to update, in parallel, at least one record in each of the stored first and second sets of records with the received data such that a previous record included in each of the first and second data structures is replaced.

2. The method of claim 1,

wherein the first and second sets of records are stored in separate first-in, first-out data structures on the data storage device; and

wherein the step of operating the processor circuitry to update at least one record in each of the stored first and second sets of records, includes the step of replacing a previous record included in each of the first and second data structures.

3. The method of claim 2, further comprising the step of:

allocating fixed amounts of storage space on the data storage device for storing each one of the first and second first-in, first-out data structures used to store the first and second sets of records.

4. The method of claim 2, wherein the first set of records include hourly records and the second set of records includes daily records.

5. The method of claim 2, further comprising the step of:

periodically collecting network traffic data;

storing the collected network traffic data in a buffer; and

operating the processor circuitry to retrieve network traffic data from the buffer, the retrieved network traffic data being received by the processor circuitry.

6. The method of claim 5,

wherein the network traffic data stored in the buffer includes time stamp information indicating the period of time in which the network traffic data was collected; and

wherein the step of operating the processor circuitry to update at least one record in each of the

stored first and second sets of records includes the step of:

examining at least one time stamp included in the buffered network traffic data.

8. The method of claim 5,

wherein the processor circuitry includes first and second central processing units, and

wherein the step of operating the processor circuitry to update at least one record in each of the stored first and second sets of records includes the step of operating the first processor to update the first set of records while operating the second processor to update the second set of records.

9. The method of claim 1,

wherein the processor circuitry includes first and second central processing units, and

wherein the step of operating the processor circuitry to update at least one record in each of the stored first and second sets of records includes the step of operating the first processor to update the first set of records while operating the second processor to update the second set of records.

10. The method of claim 5, wherein the computer system further includes a display device, the method further comprising the step of:

displaying data corresponding to overlapping periods of time at different resolutions on the display device.

11. The method of claim 1, further comprising the step of:

allocating storage space for storing the first and second sets of records in first and second first-in, first-out data structures, respectively.

12. A method of collecting and processing network traffic data, comprising the steps of:

periodically collecting network traffic data from a data probe,

generating a database of network traffic information from the collected network traffic data, the database comprising a plurality of network traffic data sets of differing degrees of data resolution corresponding to overlapping network traffic time periods,

storing each of the plurality of network traffic data sets in a different first-in, first-out data structure wherein a limited amount of data storage space is used for each of the different first-in, first out data structures,

updating, in parallel, at least one record in the different first-in, first-out data structures with the collected network traffic data, and

overwriting the oldest data records in the first-in, first-out data structure used to store one of the network traffic data sets, when the limited amount of data storage space used for said first-in, first-out data structure is filled with records.

13. The method of claim 12, wherein the differing degrees of resolution correspond to measurement time periods of different duration.

14. The method of claim 12,

wherein the collected network traffic data includes a plurality of traffic data counter values; and

wherein each traffic data counter value in the collected network traffic data includes information corresponding to an individual monitored conversation, the step of generating a database including the step of generating from the information on each different monitored conversation, a different record in each set of the plurality of network traffic data sets.

15. The method of claim 14, further comprising the step of storing each of the plurality of network traffic data sets in a different first-in, first-out data structure.

16. The method of claim 15, wherein a limited amount of data storage space is used for each of the different

first-in, first out data structures, the method further comprising the step of:

overwriting the oldest data records in the first-in, first-out data structure used to store one of the network traffic data sets, when the limited amount of data storage space used for said first-in, first-out data structure is filled with records.

17. A system for monitoring network traffic data, comprising:

a plurality of network traffic data probes for collecting network traffic information;

processor circuitry coupled to the network traffic probes for receiving data therefrom; and

a data storage device for storing a network traffic database generated by the processor circuitry using data collected by the network traffic data probes, the data storage device including:

a plurality of data structures, each data structure being a first-in, first-out data structure, each one of the plurality of data structures including network traffic data:

a) stored at a different resolution than the resolution at which network traffic data is stored in the other ones of the plurality of data structures; and

b) corresponding to a period of time which overlaps the period of time for which network traffic data is

stored in the other ones of the plurality of data structures;

means for updating, in parallel, at least one record in the different first-in, first-out data structures with the collected network traffic data, and

means for overwriting the oldest data records in the first-in, first-out data structure used to store one of the network traffic data sets, when the limited amount of data storage space used for said first-in, first-out data structure is filled with records.

18. The system of claim 17, wherein each of the plurality of data structures is a first-in, first-out data structure.

19. The system of claim 18, wherein each one of the plurality of data structures includes a plurality of data records, each data record corresponding to a monitored network conversation.

20. The system of claim 18, wherein data records are arranged within each individual data structure as a function of the time the conversation to which the record corresponds was monitored.

21. The system of claim 20, wherein records which were monitored during the same time interval are grouped together within each individual data structure.

22. The system of claim 21, further comprising:

means for modifying at least one network traffic data record included in each one of the plurality of data structures to reflect collected information about an individual network conversation.

23. The system of claim 18, further comprising:

means for modifying at least one network traffic data record included in each one of the plurality of data structures to reflect collected information about an individual network conversation.

24. The system of claim 18, wherein the processor circuitry includes a plurality of separate central processing units which operate in parallel.

25. The system of claim 24, wherein each one of the plurality of data structures includes a plurality of data records, each data record corresponding to a monitored network conversation.

26. The system of claim 24, wherein data records are arranged within each individual data structure as a function of the time the conversation to which the record corresponds was monitored.

27. The system of claim 26, wherein records which were monitored during the same time interval are grouped together within each individual data structure.

28. The system of claim 27, further comprising:

means for modifying at least one network traffic data record included in each one of the plurality of data structures to reflect collected information about an individual network conversation.

29. The system of claim 24, further comprising:

means for modifying at least one network traffic data record included in each one of the plurality of data structures to reflect collected information about an individual network conversation.

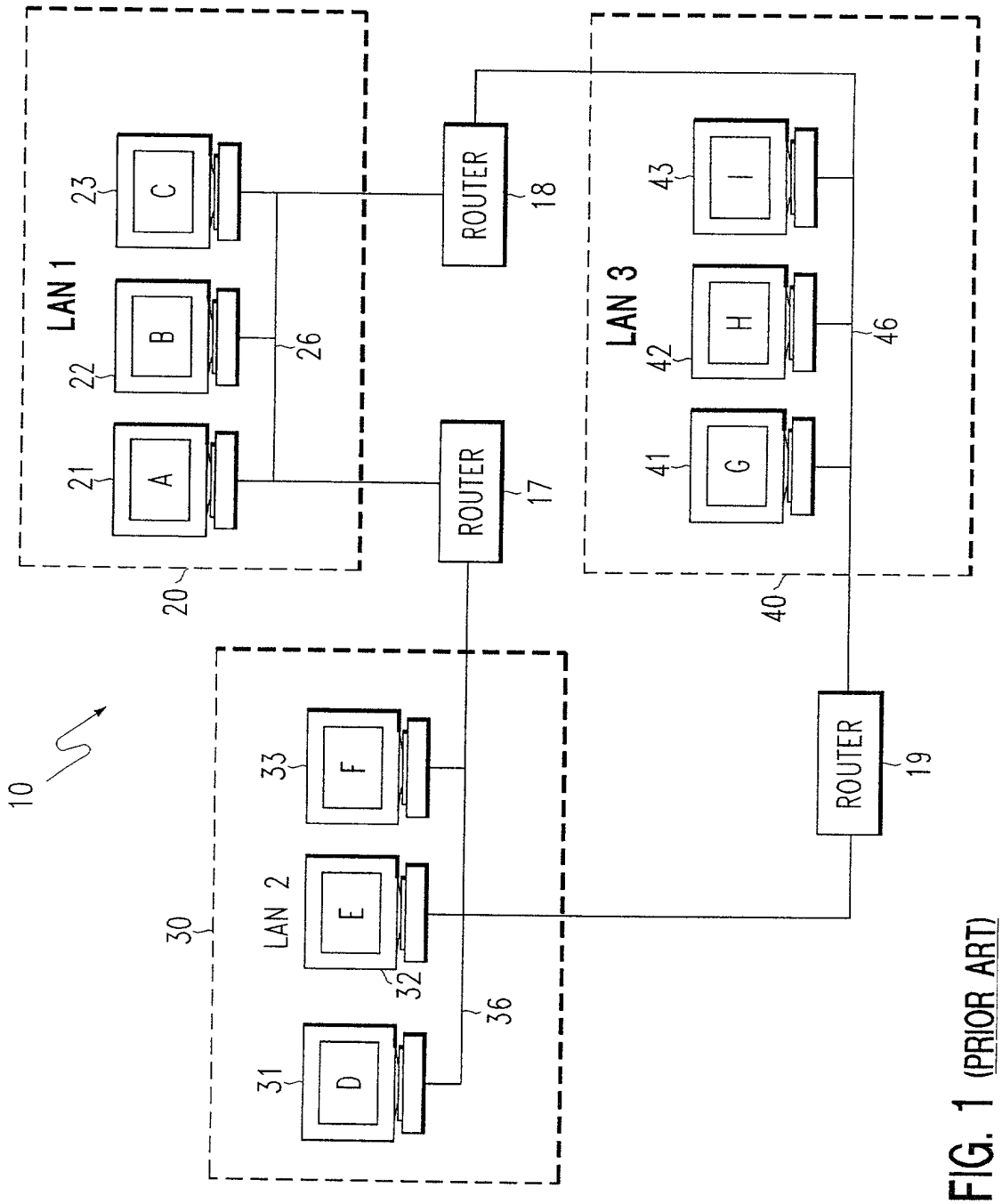


FIG. 1 (PRIOR ART)

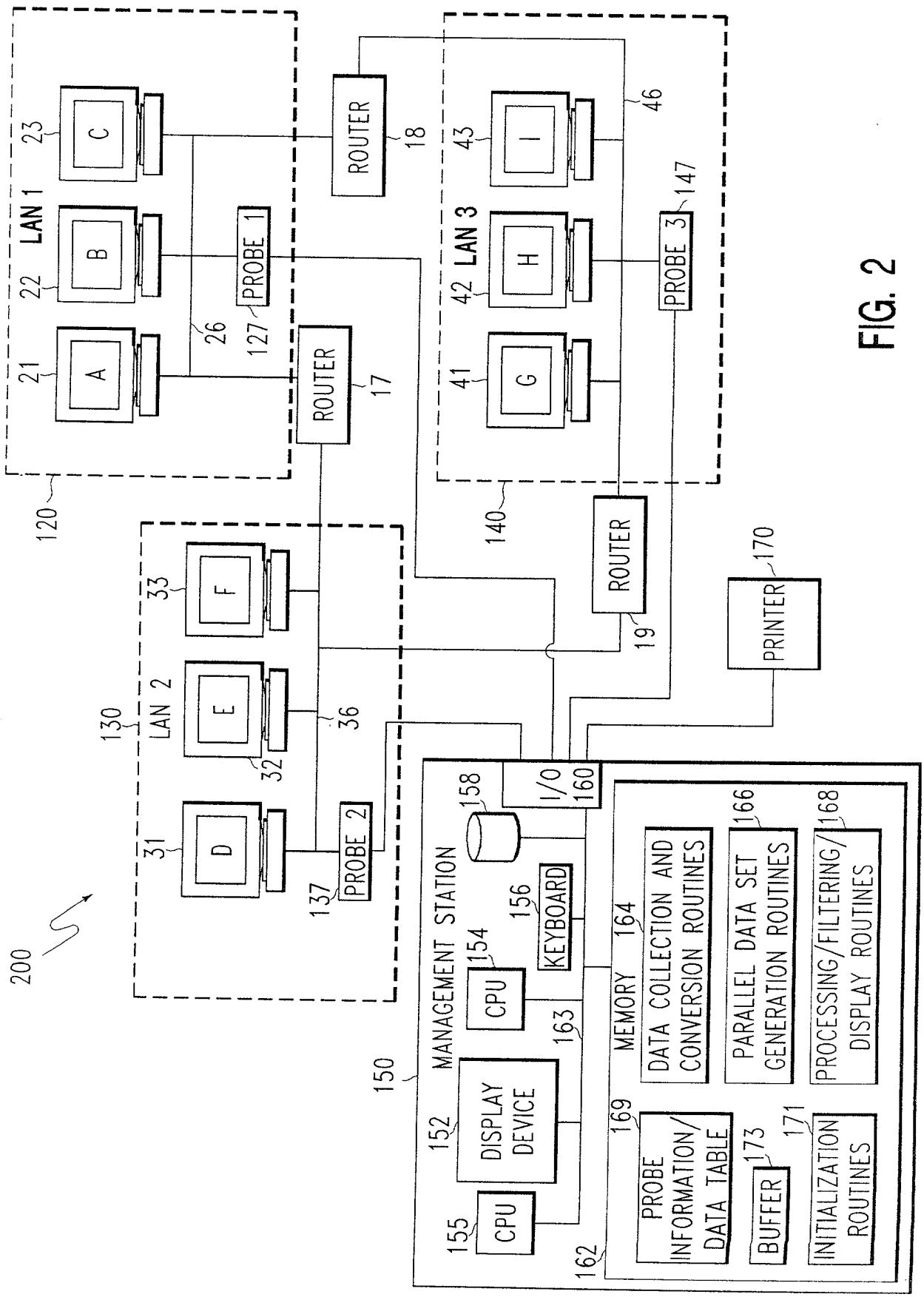

200
LAN 1
120
A
B
C
21
22
23
PROBE 1
127
26
ROUTER
17
ROUTER
18
LAN 2
130
D
E
F
31
32
33
PROBE 2
137
36
LAN 3
140
G
H
I
41
42
43
PROBE 3
147
46
ROUTER
19
PRINTER
170
MANAGEMENT STATION
150
I/O
160
158
CPU
154
KEYBOARD
156
163
DISPLAY DEVICE
152
CPU
155
MEMORY
164
162
DATA COLLECTION AND CONVERSION ROUTINES
PARALLEL DATA SET GENERATION ROUTINES
166
PROCESSING/FILTERING/ DISPLAY ROUTINES
168
PROBE INFORMATION/ DATA TABLE
169
BUFFER
173
INITIALIZATION ROUTINES
171

FIG. 2

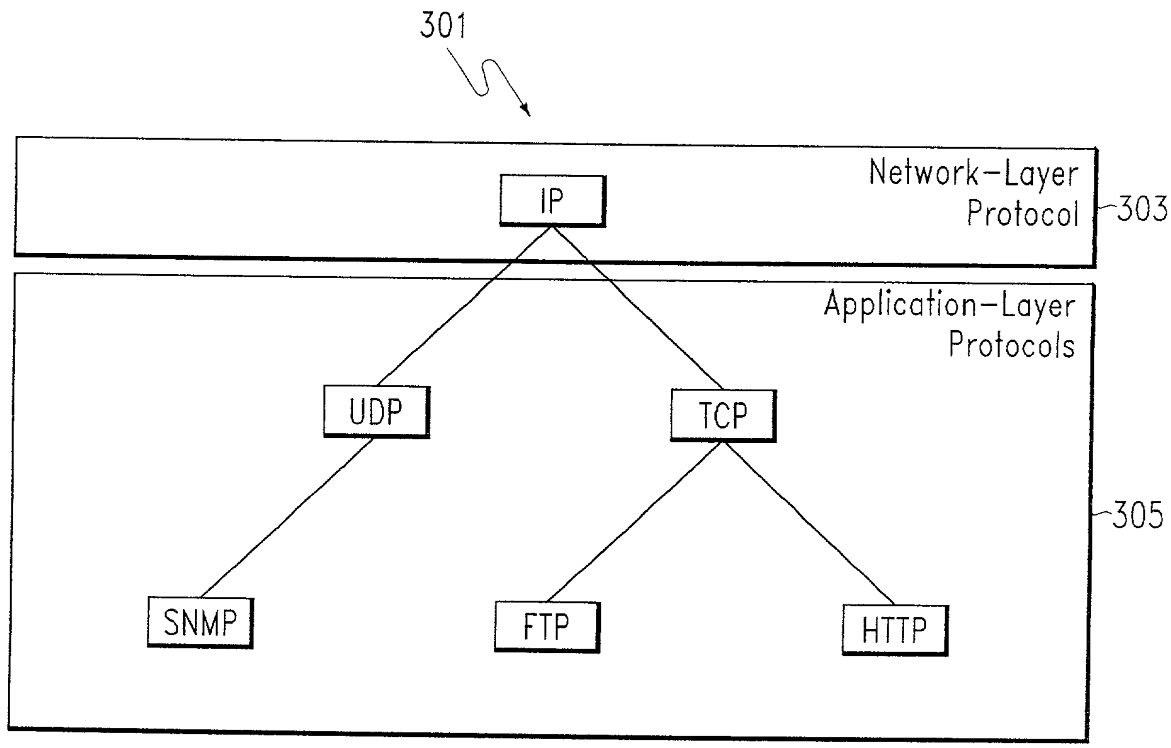


FIG. 3

169

PROBE IDENTIFIER	PROBE DATA TABLE FORMAT	TEMPORARY DATA TABLE STORAGE
PROBE 1 127	alMatrixTopN(All Count Mode)	TEMPORARY DATA TABLE STORAGE
PROBE 2 137	alMatrix	TEMPORARY DATA TABLE STORAGE
PROBE 3 147	nlMntrix	TEMPORARY DATA TABLE STORAGE

FIG. 4B

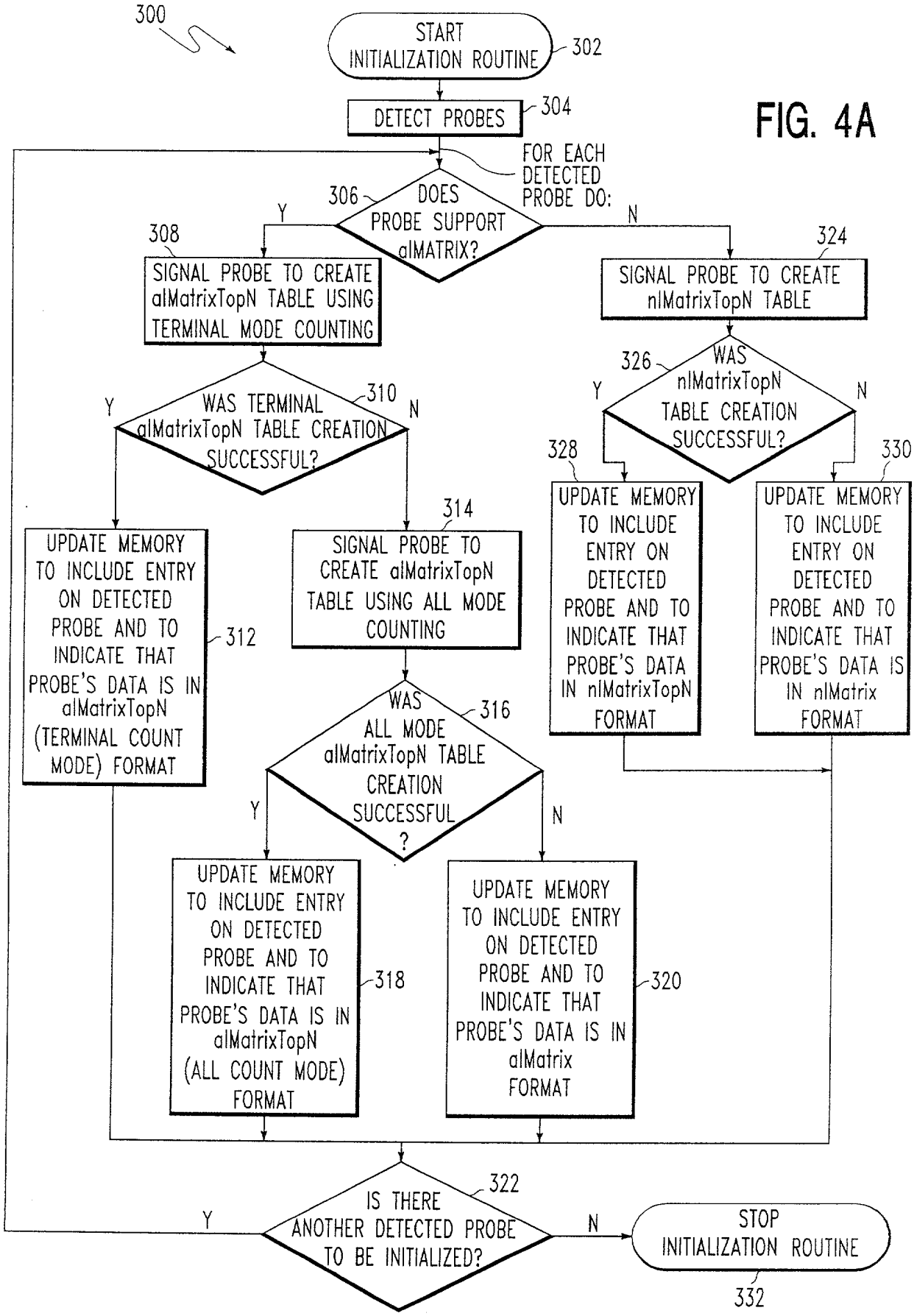


FIG. 4A

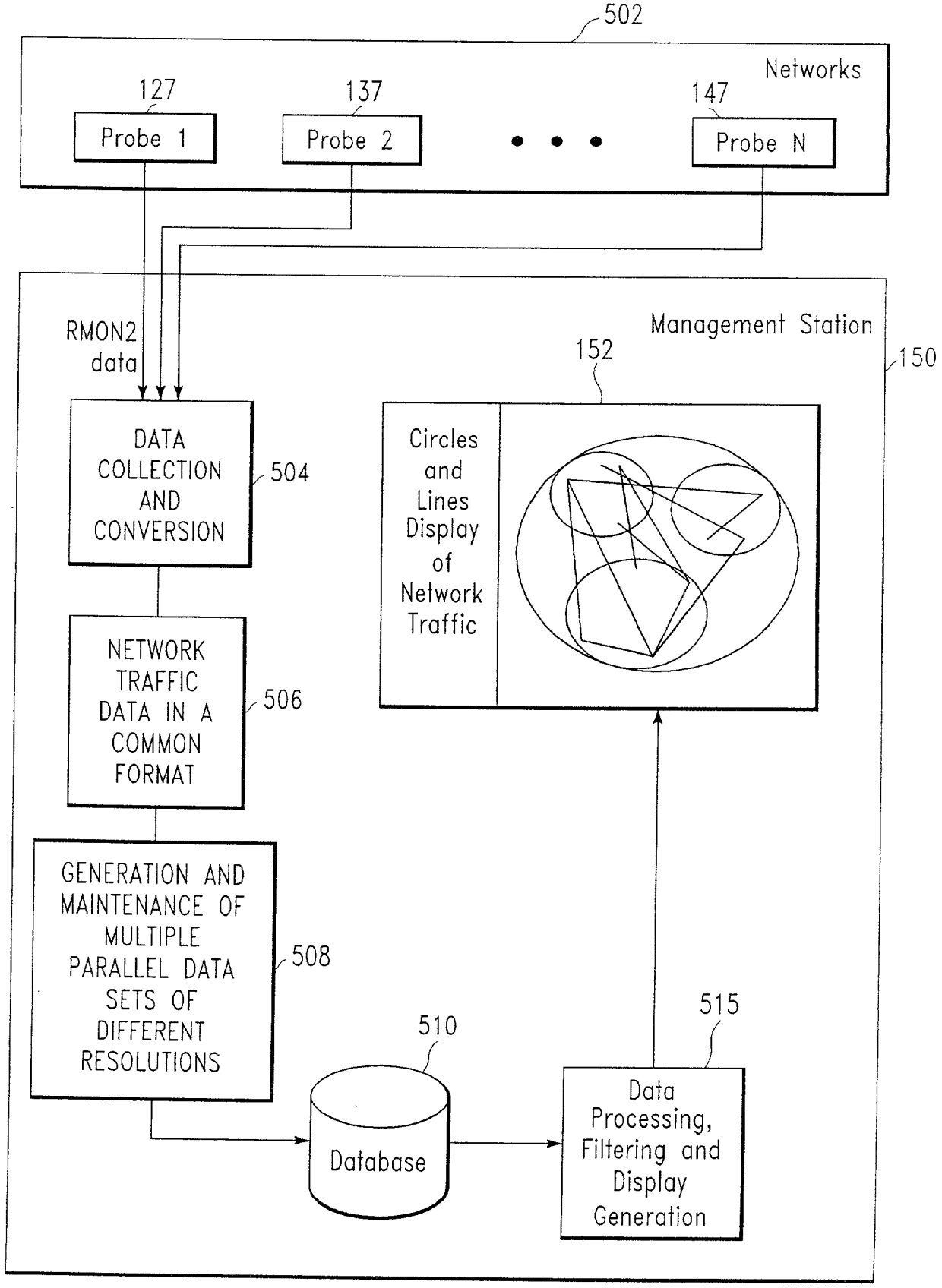

502
Networks
127
Probe 1
137
Probe 2
147
Probe N
RMON2 data
Management Station
150
152
DATA COLLECTION AND CONVERSION
504
Circles and Lines Display of Network Traffic
NETWORK TRAFFIC DATA IN A COMMON FORMAT
506
GENERATION AND MAINTENANCE OF MULTIPLE PARALLEL DATA SETS OF DIFFERENT RESOLUTIONS
508
510
515
Database
Data Processing, Filtering and Display Generation

FIG. 5

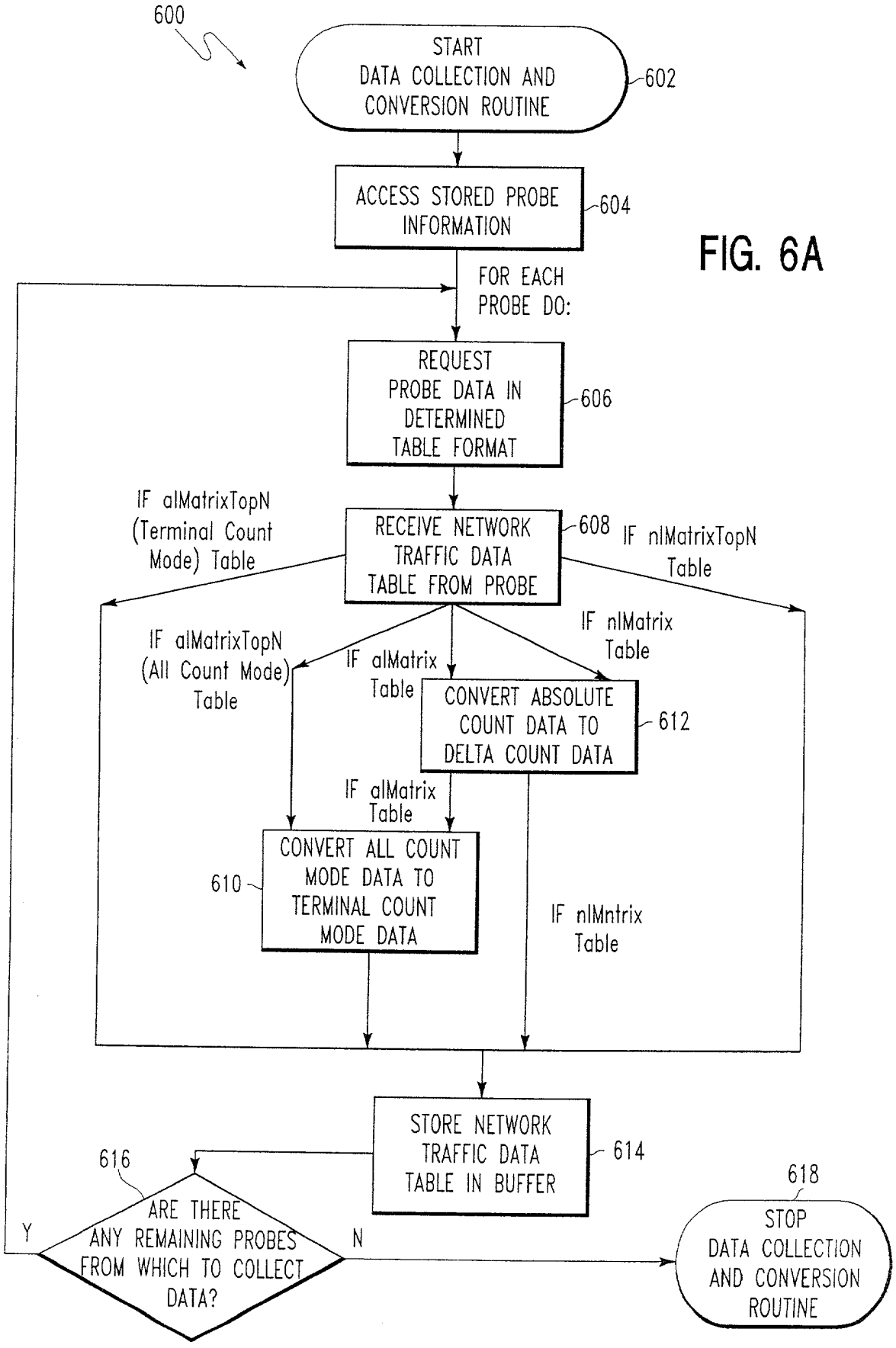


FIG. 6A

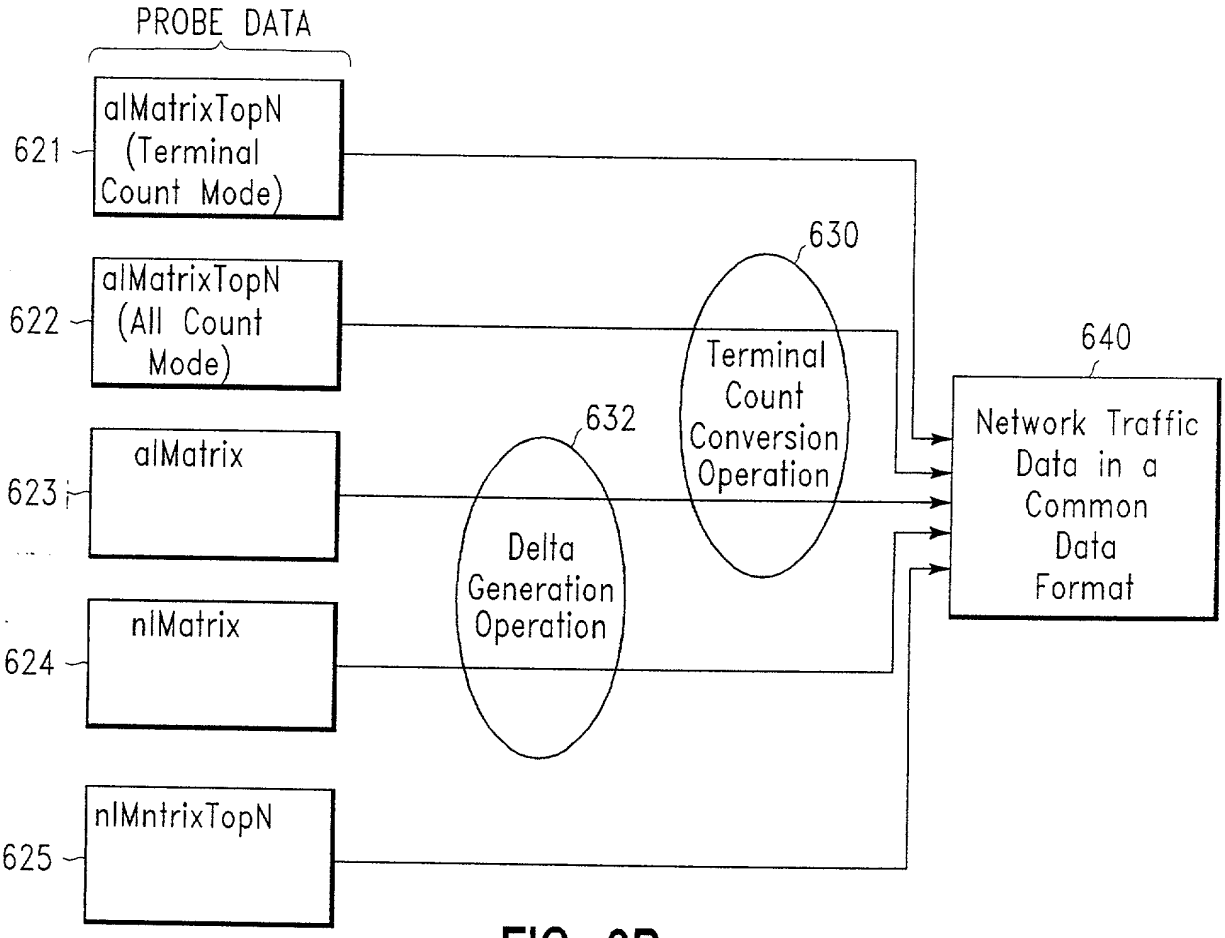

PROBE DATA
621
alMatrixTopN (Terminal Count Mode)
622
alMatrixTopN (All Count Mode)
623
alMatrix
624
nlMatrix
625
nlMntrixTopN
630
Terminal Count Conversion Operation
632
Delta Generation Operation
640
Network Traffic Data in a Common Data Format

FIG. 6B

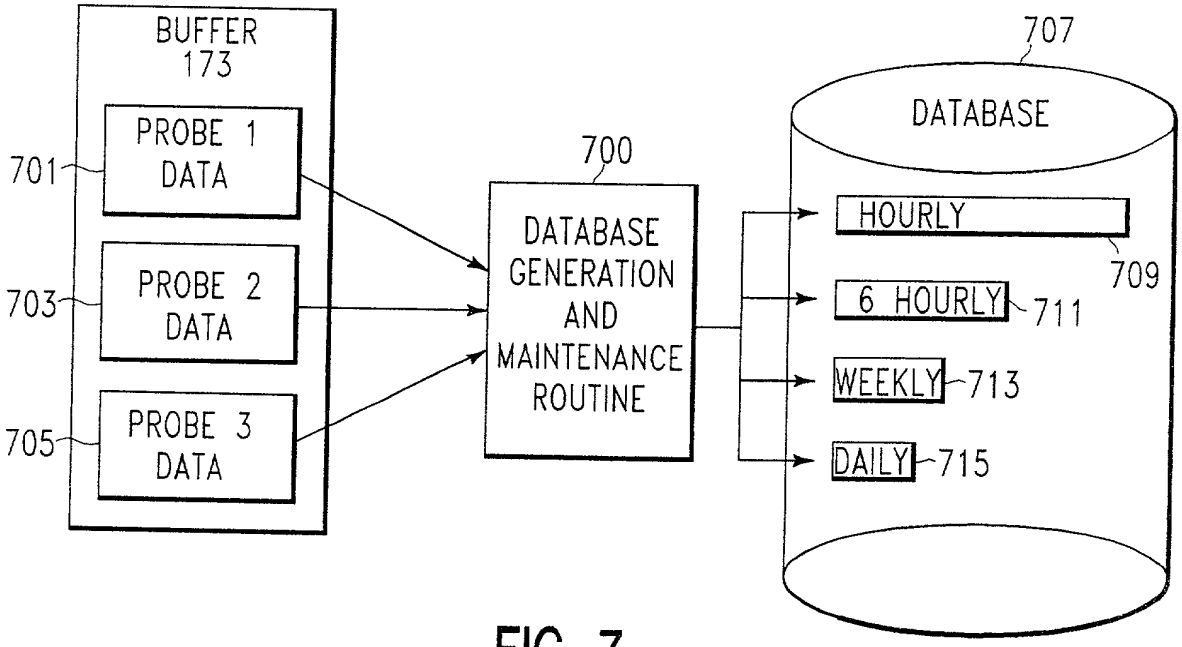

BUFFER 173
701
PROBE 1 DATA
703
PROBE 2 DATA
705
PROBE 3 DATA
700
DATABASE GENERATION AND MAINTENANCE ROUTINE
707
DATABASE
HOURLY
709
6 HOURLY
711
WEEKLY
713
DAILY
715

FIG. 7

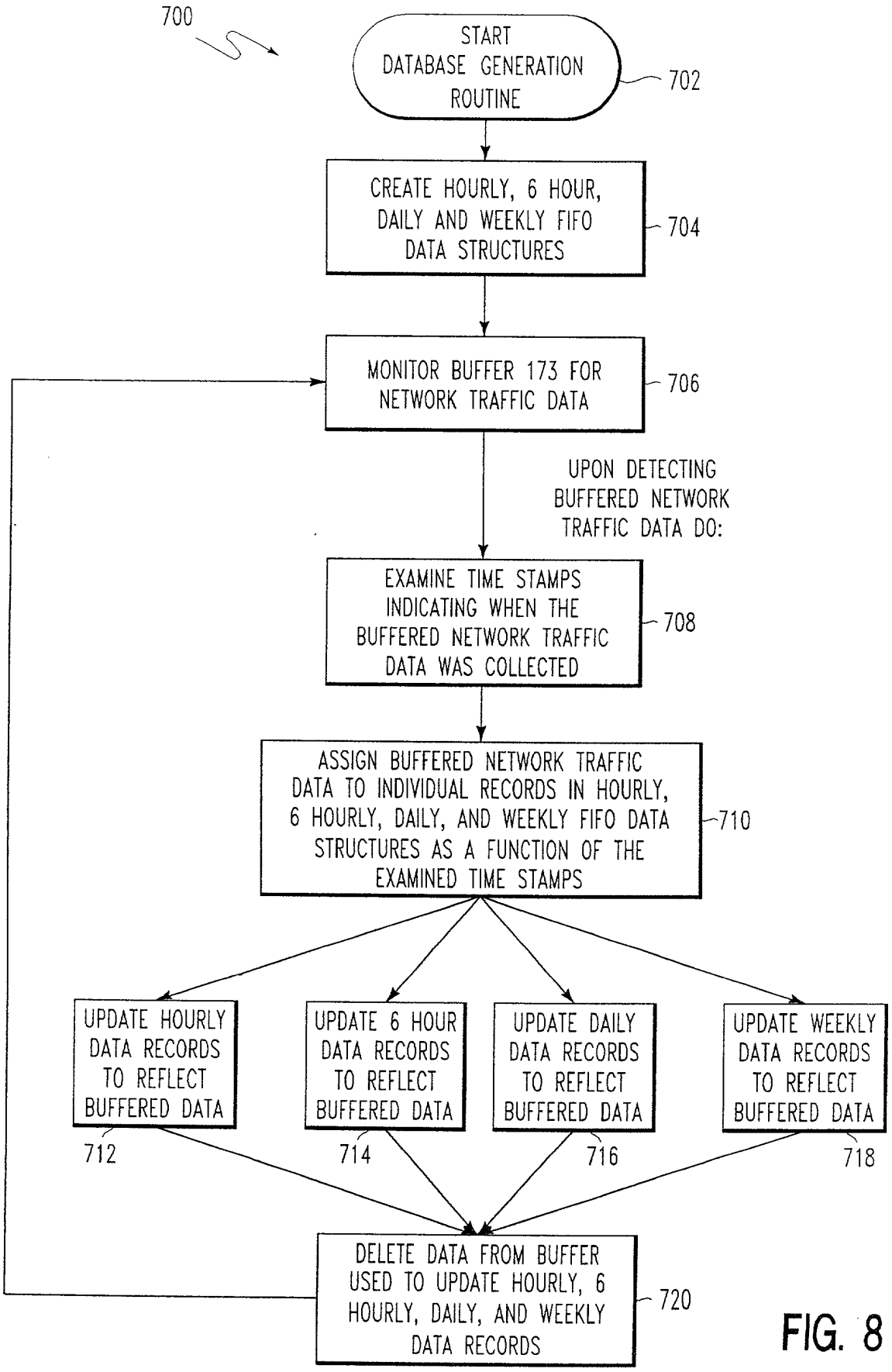

700
START DATABASE GENERATION ROUTINE
702
CREATE HOURLY, 6 HOUR, DAILY AND WEEKLY FIFO DATA STRUCTURES
704
MONITOR BUFFER 173 FOR NETWORK TRAFFIC DATA
706
UPON DETECTING BUFFERED NETWORK TRAFFIC DATA DO:
EXAMINE TIME STAMPS INDICATING WHEN THE BUFFERED NETWORK TRAFFIC DATA WAS COLLECTED
708
ASSIGN BUFFERED NETWORK TRAFFIC DATA TO INDIVIDUAL RECORDS IN HOURLY, 6 HOURLY, DAILY, AND WEEKLY FIFO DATA STRUCTURES AS A FUNCTION OF THE EXAMINED TIME STAMPS
710
UPDATE HOURLY DATA RECORDS TO REFLECT BUFFERED DATA
712
UPDATE 6 HOUR DATA RECORDS TO REFLECT BUFFERED DATA
714
UPDATE DAILY DATA RECORDS TO REFLECT BUFFERED DATA
716
UPDATE WEEKLY DATA RECORDS TO REFLECT BUFFERED DATA
718
DELETE DATA FROM BUFFER USED TO UPDATE HOURLY, 6 HOURLY, DAILY, AND WEEKLY DATA RECORDS
720

FIG. 8

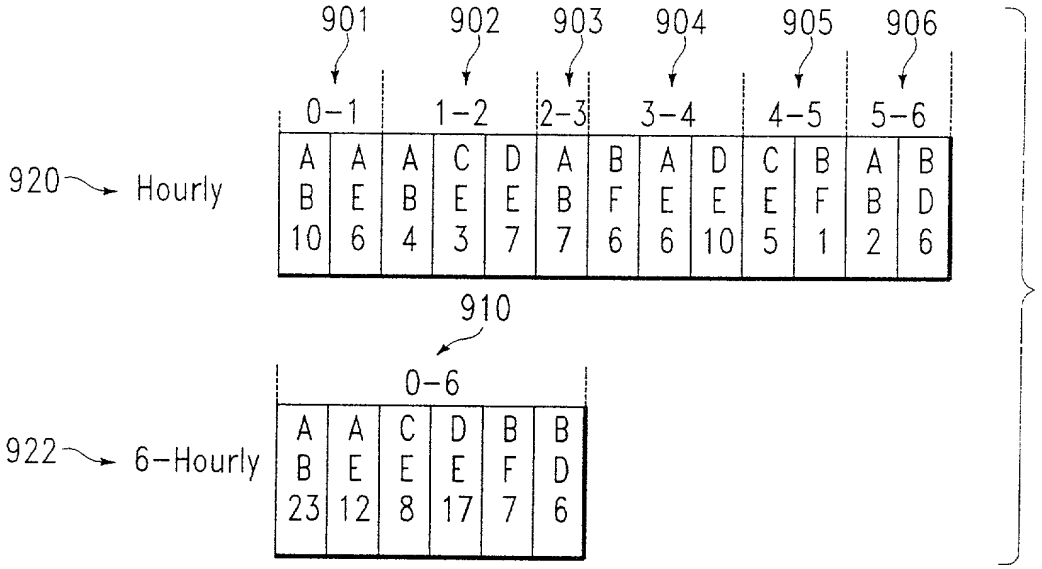

901
902
903
904
905
906
0–1
1–2
2–3
3–4
4–5
5–6
920
Hourly
A B 10
A E 6
A B 4
C E 3
D E 7
A B 7
B F 6
A E 6
D E 10
C E 5
B F 1
A B 2
B D 6
910
0–6
922
6–Hourly
A B 23
A E 12
C E 8
D E 17
B F 7
B D 6

FIG. 9

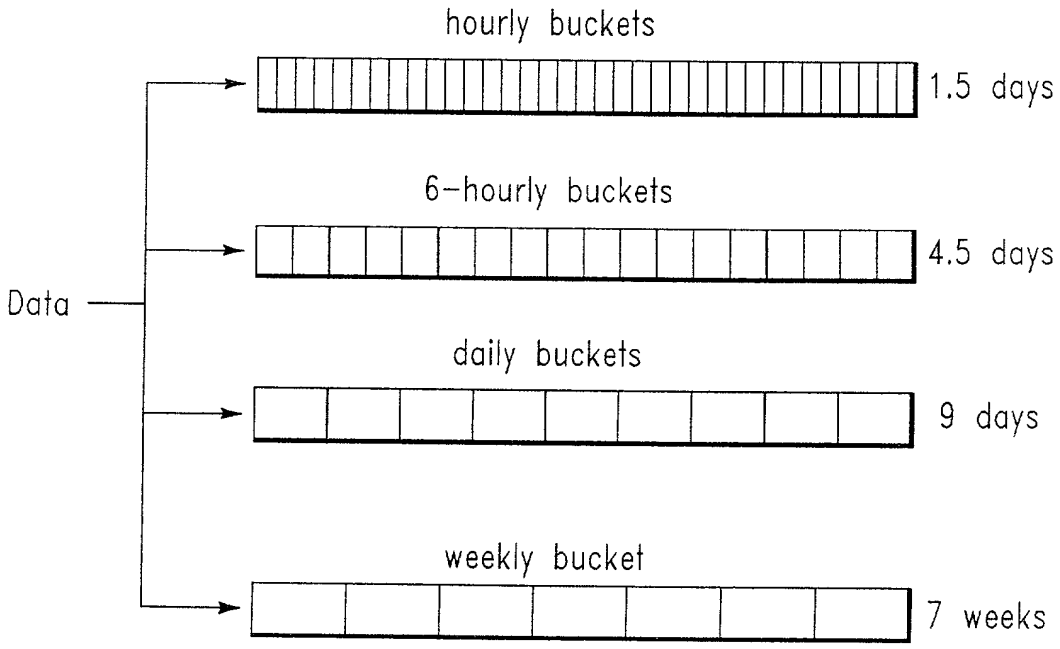

hourly buckets
1.5 days
6–hourly buckets
4.5 days
Data
daily buckets
9 days
weekly bucket
7 weeks

FIG. 10